Google Inc. et al v. Egger et al Doc. 155

Elizabeth J. Cabraser (State Bar No. 083151)
Barry R. Himmelstein (State Bar No. 157736)
Michael W. Sobol (State Bar No. 194857)
Eric B. Fastiff (State Bar No. 182260)
Allison S. Elgart (State Bar No. 241901)
LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP
275 Battery Street, 30th Floor
San Francisco, CA 94111-3339
Telephone: (415) 956-1000
Facsimile: (415) 956-1008

Interim Class Counsel for MCI Class

[Additional Counsel Appear On Signature Page]

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

(San Francisco Division)

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION THIS DOCUMENT RELATES TO: All Class Actions Against MCI, Verizon, Sprint, BellSouth, Cingular, and Transworld Defendants *Campbell v. AT&T Communications of California* (No. 06-3596); *Riordan v. Verizon Communications, Inc.* (No. 06-3574)	MDL Docket No. 06-1791 (VRW) **CLASS PLAINTIFFS' CONSOLIDATED RESPONSE TO ORDER TO SHOW CAUSE WHY RULINGS ON *HEPTING* MOTIONS TO DISMISS SHOULD NOT APPLY** Date: February 9, 2007 Time: 2:00 p.m. Courtroom: 6, 17th Floor Judge: Hon. Vaughn R. Walker

Dockets.Justia.com

TABLE OF CONTENTS

Page

I. INTRODUCTION 1

II. THE MASTER COMPLAINTS 2

A. The Common, Federal Claims 3

B. The State Law Claims 4

III. THE FACTUAL RECORD 7

A. Publicly Disclosed Information About the NSA Surveillance Program That Was Before The Court in *Hepting* 7

B. Statements By Members of Congress Who Have Been Briefed on the Call Records Program 9

C. Additional Public Disclosures Not Discussed in *Hepting* 14

IV. WITH ONE EXCEPTION, THE COURT'S RULINGS ON THE STATE SECRETS ISSUES IN *HEPTING* ARE EQUALLY APPLICABLE HERE 17

A. The Categorical *Totten/Tenet* Bar Does Not Apply 19

B. The Very Subject Matter of the Actions is Not a State Secret 20

C. Dismissal on Evidentiary Grounds Would Be Premature 20

D. The Existence or Non-Existence of a Certification Is Not a State Secret 21

E. The Statutory Privileges Do Not Warrant Dismissal 21

V. ADDITIONAL INFORMATION CONFIRMS THAT THE RECORDS PROGRAM IS NOT A SECRET 22

A. The Court's Ruling in *Hepting* 22

B. The Existence of The Records Program Has Been Acknowledged by Nineteen Members of Congress Briefed on the Program by the NSA 23

C. Verizon Has Tacitly Admitted That MCI Participated in the Records Program 27

D. Discovery Concerning the Existence of Any Certifications Concerning the Records Program Received by Verizon and/or BellSouth Must Be Permitted 28

E. The Wholesale Violation of Federal Privacy Laws Cannot Be a "State Secret" 29

VI. THE COURT'S RULINGS ON AT&T'S MOTION TO DISMISS ARE EQUALLY APPLICABLE HERE 30

A. Plaintiffs Have Standing to Pursue Their Claims 30

B. Plaintiffs Have Alleged the Absence of a Certification 31

C. Defendants Have No Common Law Immunity 32

D. Defendants Have No Qualified Immunity 33

VII. CONCLUSION 34

TABLE OF AUTHORITIES

Page

CASES

Ballard v. Equifax Check Services, Inc., 158 F. Supp. 2d 1163 (E.D. Cal. 2001) 4

Diaz v. Allstate Ins. Group, 185 F.R.D. 581 (C.D. Cal. 1998) 4

Hepting v. AT&T Corp., 439 F. Supp. 2d 974 (N.D. Cal. 2006) .... passim

Hope v. Pelzer, 536 U.S. 730 (2002) 33

Jabara v. Kelley, 75 F.R.D. 475 (E.D. Mich. 1977) 24

Tenet v. Doe, 544 U.S. 1 (2005) 19

Terkel v. AT&T Corp., 441 F. Supp. 2d 899 (N.D. Ill. 2006) .... *passim*

Totten v. United States, 92 U.S. 105 (1876) 19

United States v. United States District Court, 407 U.S. 297 (1972) 33

STATUTES

18 U.S.C. § 2511 32

18 U.S.C. § 2518 32

18 U.S.C. § 2520 31

18 U.S.C. § 2703 32

28 U.S.C. § 1407 1

50 U.S.C. § 402 *note* 21

50 U.S.C. § 403 22

RULES

Federal Rules of Evidence, Rule 104(a) 22

TREATISES

Manual For Complex Litigation, Fourth (2004) 1

I. INTRODUCTION

This multidistrict litigation ("MDL") proceeding includes cases brought by and on behalf of customers and subscribers of the largest telecommunications carriers in the United States, including the three primary long distance carriers, AT&T, MCI, and Sprint,[1] as well as "Baby Bells" Verizon and BellSouth, a number of wireless carriers, and their respective affiliates. In each case, Plaintiffs[2] allege that the defendant carriers, acting at the request of the National Security Agency ("NSA"), have unlawfully given the federal government access to: (1) the domestic and international telephone calls of their customers, including Plaintiffs (the "content" claims); and (2) records of the date, time, number dialed, and duration of those calls (the "records" claims).

In *Hepting v. AT&T Corp.*, 439 F. Supp. 2d 974 (N.D. Cal. 2006) ("*Hepting*"), the Court denied the government's motion to dismiss or for summary judgment based on the state secrets privilege, and denied AT&T Corp.'s ("AT&T's") motion to dismiss based on lack of standing, failure to plead the absence of a certification, common law immunity, and qualified immunity. On November 22, 2006, the Court issued Pretrial Order No. 1, requiring, *inter alia*, "[a]ll parties to SHOW CAUSE in writing why the *Hepting* order should not apply to all cases and claims to which the government asserts the state secrets privilege" (the "OSC").[3] Plaintiffs take issue with but one of the Court's many rulings in *Hepting*: that "unlike the program monitoring communication content, the general contours and even the existence of the communication records program remain unclear." *Id.* at 997.

---

[1] In 2003, AT&T received 30.0% of all long distance toll service revenues, MCI received 20.8%, and Sprint, 8.2%; AT&T had residential long distance market share of 31.7%, MCI 13.0%, and Sprint 7.1%. Federal Communications Commission, Industry Analysis and Technology Division, Wireline Competition Bureau, *Trends in Telephone Service* (June 21, 2005), Tables 9.6, 9.7 (available at http://www.fcc.gov/Bureaus/Common_Carrier/Reports/FCC-State_Link/IAD/trend605.pdf).

[2] Unless otherwise noted, "Plaintiffs" and "Defendants" refer to the named plaintiffs and defendants in the coordinated actions generally.

[3] The OSC is well within the statutory mandate of an MDL transferee judge to "promote the just and efficient conduct" of coordinated actions. 28 U.S.C. § 1407(a). Indeed, the "Bible" on MDL proceedings, the Federal Judicial Center's *Manual for Complex Litigation, Fourth* (2004), expressly directs that "[o]rdinarily, it is advisable to order that . . . rulings on common issues—for example, on the statute of limitations—shall be deemed to have been made in the tag-along action[s] without the need for separate motions and orders . . . ." *Id.* at § 20.132, p. 222-23.

The existence and general contours of the records program have been acknowledged by numerous members of the Congressional intelligence oversight committees briefed on the program by the NSA, and at least one carrier, Verizon, has tacitly admitted the participation of its newly-acquired subsidiary, MCI, in the records program. Accordingly, the records program is no longer a secret, and Plaintiffs should be permitted discovery on their records claims.

II. THE MASTER COMPLAINTS

Pursuant to Pretrial Order No. 1 (Dkt. No. 79), Plaintiffs' List of Interim Class Counsel for Each Defendant Category (Dkt. No. 88), and the Court's Order Resetting Deadlines (Dkt. No. 112), on January 16, 2007, Plaintiffs filed five master complaints (collectively, the "Master Complaints") against the various defendant groups as follows: (1) Master Consolidated Complaint Against MCI Defendants[4] and Verizon Defendants[5] (Dkt. No. 125, "MCI/Verizon Master Compl."); (2) Master Consolidated Complaint Against Defendants Sprint Nextel Corporation, Sprint Communications Co. Ltd. Partnership, Nextel Communications, Inc., Embarq Corporation, UCOM, Inc., U.S. Telecom, Inc., Utelcom, Inc., and Does 1-100 for Damages, Declaratory and Equitable Relief (Dkt. No. 124, "Sprint Master Compl."); (3) Master Consolidated Complaint Against Defendant "BellSouth"[6] for Damages, Declaratory and Equitable Relief (Dkt. No. 126, "BellSouth Master Compl."); (4) Master Consolidated Complaint Against Defendants Transworld Network Corp., Comcast Telecommunications, Inc., T-Mobile USA, Inc., and McLeodUSA Telecommunications Services, Inc., for Damages, Declaratory and Equitable Relief (Dkt. No. 125, "Transworld Master Compl."); and (5) Master Consolidated

---

[4] Defendants MCI Communications Services, Inc. and MCI, LLC.

[5] Defendants Verizon Communications, Inc., Verizon California, Inc., Verizon Delaware, Inc., Verizon Florida, Inc., Verizon Maryland Inc., Verizon New England, Inc., Verizon New Jersey, Inc., Verizon New York, Inc., Verizon North, Inc., Verizon Northwest, Inc., Verizon Pennsylvania, Inc., Verizon South, Inc., Verizon Virginia, Inc., Verizon Washington, D.C., Inc., Verizon West Virginia, Inc., GTE Corporation, GTE Southwest Incorporates, Contel of the South, Inc., Verizon Federal, Inc., Bell Atlantic Communications, Inc., Verizon Select Services, Inc., NYNEX Long Distance Company, Verizon Business Network Services, Inc., Cellco Partnership, NYNEX Corporation, GTE Wireless, Inc., GTE Wireless of the South, Inc., NYNEX PCS, Inc., and Verizon Wireless of the East LP.

[6] Defendants BellSouth, BellSouth Communications, LLC, BellSouth Corp., BellSouth Corporation, BellSouth Telecommunications, Inc., and AT&T Southeast.

Complaint Against Defendants AT&T Mobility LLC (f/k/a Cingular Wireless, L.L.C.), Cingular Wireless Corp., and New Cingular Wireless Services, Inc. for Damages, Declaratory and Equitable Relief (Dkt. No. 121, "Cingular Master Compl.").[7]

The facts and claims alleged, and their substantial overlap with the facts and claims alleged in *Hepting*, are summarized below.

A. The Common, Federal Claims

Like the *Hepting* complaint, the Master Complaints assert federal constitutional and statutory claims for violations of:

> (1) The First and Fourth Amendments to the United States Constitution (acting as agents or instruments of the government) by illegally intercepting, disclosing, divulging and/or using plaintiffs' communications;[8]
>
> (2) Section 109 of Title I of the Foreign Intelligence Surveillance Act of 1978 (FISA), 50 U.S.C. § 1809, by engaging in illegal electronic surveillance of plaintiffs' communications under color of law;[9]
>
> (3) Section 802 of Title III of the Omnibus Crime Control and Safe Streets Act of 1968, as amended by section 101 of Title I of the Electronic Communications Privacy Act of 1986 (ECPA), 18 U.S.C. §§ 2511(1)(a), (1)(c), (1)(d) and (3)(a), by illegally intercepting, disclosing, using and/or divulging plaintiffs' communications;[10]
>
> (4) Section 705 of Title VII of the Communications Act of 1934, as amended, 47 U.S.C. § 605, by unauthorized divulgence and/or publication of plaintiffs' communications;[11]
>
> (5) Section 201 of Title II of the ECPA ("Stored Communications Act"), as amended, 18 U.S.C. §§ 2702(a)(1) and (a)(2), by illegally divulging the contents of plaintiffs' communications;[12]
>
> (6) Section 201 of the Stored Communications Act, as amended by section 212 of Title II of the USA PATRIOT Act, 18 U.S.C. § 2702(a)(3), by illegally divulging records concerning plaintiffs'

---

[7] The operative complaint in *Hepting* (*Hepting* Dkt. No. 8) has been designated the lead complaint for the AT&T defendant group. *See* Transcript, Nov. 17, 2006 Case Management Conference, at 79:6-17.

[8] *See* Sixth Claim for Relief in each of the Master Complaints.

[9] *See* Fifth Claim for Relief in each of the Master Complaints.

[10] *See* Third Claim for Relief in each of the Master Complaints.

[11] *See* Fourth Claim for Relief in each of the Master Complaints.

[12] *See* First Claim for Relief in each of the Master Complaints.

communications to a governmental entity[;][13] and

(7) California's Unfair Competition Law, Cal Bus & Prof Code §§ 17200 et seq., by engaging in unfair, unlawful and deceptive business practices.[14]

439 F. Supp. 2d at 978-79 (listing claims asserted in *Hepting*).

B. The State Law Claims

In addition to the claims asserted in *Hepting*, the Master Complaints assert several claims for relief arising under state law, specifically: (1) violation of the surveillance statutes of all States and the District of Columbia;[15] (2) violation of the consumer protection statutes of all States and the District of Columbia, based, *inter alia*, on Defendants' violation of their own privacy policies, which falsely assured customers that Defendants would not divulge their customers' communications or records except as required by law;[16] and (3) common law breach of contract, based on the violation of Defendants' privacy policies.[17] The BellSouth, Sprint, and Cingular Master Complaints also assert breach of warranty claims.[18] The BellSouth Master Complaint also asserts claims for violation of the right of privacy under the California Constitution[19] and violation of Cal. Penal Code § 11149.4.[20] The Cingular Master Complaint also asserts claims for relief for: (1) violation of the Hawaii Constitution, Article I, Section 6;[21] (2) violation of the New Jersey Constitution;[22] (3) malicious misrepresentation;[23] (4) invasion of privacy under New Jersey law;[24] (5) violations of the Truth-in-Consumer Contract, Warranty and Notice Act;[25] (6) violations of N.J.S.A. 2C:21-7 and 2C:21-17.3;[26] and (7) invasion of privacy under Texas law.[27] The *Campbell*[28] and *Riordan*[29] cases, which the Court has declined to remand, assert only non-class claims for declaratory and injunctive relief under the California Constitution and California Public Utilities Code Section 2891 against several AT&T defendants and a Verizon defendant, respectively. These non-class claims are proceeding in parallel with the Master Complaints.

---

[13] *See* Second Claim for Relief in each of the Master Complaints.

[14] *See* Tenth Claim for Relief, MCI/Verizon Master Compl.; Ninth Claim for Relief, BellSouth Master Compl.; Ninth Claim for Relief, Transworld Master Compl.; Twenty-Third Claim for Relief, ¶ 265(e), Cingular Master Compl. This claim alleges, *inter alia*, that Defendants engaged in unlawful business practices by violating the Pen Register Act, 18 U.S.C. § 3121, *et seq*., as well as 47 U.S.C. § 222(c), which requires Defendants to maintain the confidentiality of customer proprietary network information. While neither of these federal statutes provide for a private right of action, it is well-settled that violations of such federal statutes remain actionable as "unlawful business practices" in violation of California's Unfair Competition Law. *See Diaz v. Allstate Ins. Group*, 185 F.R.D. 581, 594 (C.D. Cal. 1998) ("Under California law, a private plaintiff may bring action under unfair competition statute to redress any unlawful business practice, including those that do not otherwise permit a private right of action") (citation omitted); *Ballard v. Equifax Check Services, Inc.*, 158 F. Supp. 2d 1163, 1176 (E.D. Cal. 2001) (violation of virtually any federal law may constitute unlawful business practice actionable under Cal. Unfair Competition Law).

[15] Ala. Code §§ 13A-11-30, 13A-11-31; Alaska Stat. § 42.20.310; Ariz. Rev. Stat. Ann. § 13-3005; Ark. Code Ann. § 5-60-120; Cal. Penal Code § 630 *et seq.*; Colo. Rev. Stat. §§ 18-9-301, 18-9-303; Conn. Gen. Stat. § 52-570d; Del. Code Ann. Tit. 11, § 2402; D.C. Code §§ 23-541, 23-542; Fla. Stat. §§ 934.01-03; Ga. Code Ann. §§ 16-11-62 *et seq.*; Haw. Rev. Stat. § 803-42, 803-48 (2005); Idaho Code Ann. § 18-6702; 720 Ill. Comp. Stat. 5/14-1, -2; Ind. Code § 35-33.5-1 *et seq.*; Iowa Code § 727.8; Kan. Stat. Ann. §§ 21-4001, 21-4002; Ky. Rev. Stat. Ann. §§ 526.010-.020; La. Rev. Stat. Ann. § 15:1303; Me. Rev. Stat. Ann. Tit. 15, §§ 709-710; Md. Code Ann. Cts. & Jud. Proc. § 10-402 *et seq.*; § 10-4A-4B *et seq.*; Mass. Gen. Laws ch. 272, § 99; Mich. Comp. Laws § 750.539 *et seq.*; Minn. Stat. §§ 626A.01, .02; Miss. Code Ann. § 41-29-501 *et seq.*; Mo. Rev. Stat. §§ 392.170, .350, 542.402, .418; Mont. Code Ann. § 45-8-213; Neb. Rev. Stat. § 86-290; Nev. Rev. Stat. 200.610-.620; N.H. Rev. Stat. Ann. §§ 570-A:1, -A:2; N.J. Stat. Ann. § 2A:156A-1 *et seq.*; N.M. Stat. § 30-12-1; N.Y. Penal Law §§ 250.00, .05; N.C. Gen. Stat. § 15A-287; N.D. Cent. Code § 12.1-15-02; Ohio Rev. Code Ann. § 2933.51 *et seq.*; Okla. Stat. tit. 13, § 176.1 *et seq.*; Or. Rev. Stat. §§ 165.540, .543; 18 Pa. Cons. Stat. § 5701 *et seq.*; R.I. Gen. Laws § 11-35-21; S.C. Code Ann. §§ 17-30-20, -30; S.D. Codified Laws §§ 23A-35A-1, 23A-35A-20; Tenn. Code Ann. § 39-13-601; Tex. Penal Code Ann. § 16.02 *et seq.*; Tex. Code Crim. Proc. art. 18.20 § 16(a); Utah Code Ann. § 77-23a-1 *et seq.*; Va. Code Ann. §§ 19.2-61, -62; Wash. Rev. Code § 9.73.030; W. Va. Code § 62-1D-1 *et seq.*; Wis. Stat. §§ 968.27, .31; Wyo. Stat. Ann. §§ 7-3-701, -702. *See* Seventh Claim for Relief in MCI/Verizon, BellSouth, and Transworld Master Complaints; Seventh and Eleventh Claims for Relief, Sprint Master Compl.; Seventh, Eighth, Eleventh, Twelfth, Twentieth, and Twenty-Second Claims for Relief, Cingular Master Compl.

---

[16] Ala. Code § 8-19-1 *et seq.*; Ariz. Rev. Stat. § 44-1522 *et seq.*; Ark. Code § 4-88-101 *et seq.*; Cal. Bus. & Prof. Code § 17200 *et seq.*; Colo. Rev. Stat. § 6-1-105 *et seq.*; Conn. Gen. Stat. § 42-110b *et seq.*; 6 Del. Code § 2511 *et seq.*; D.C. Code Ann. § 28-3901 *et seq.*; Fla. Stat. § 501.201 *et seq.*; Ga. Stat. § 10-1-392 *et seq.*; Haw. Rev. Stat. § 480 *et seq.*; Idaho Code § 48-601 *et seq.*; 815 Ill. Comp. Stat. § 505.1 *et seq.*; Ind. Code § 24-5-0.5 *et seq.*; Iowa Code § 714.16 *et seq.*; Kan. Stat. Ann. § 50-623 *et seq.*; Ky. Rev. Stat. § 367.1 10 *et seq.*; La. Rev. Stat. § 51:1401 *et seq.*; 5 Me. Rev. Stat. Ann. § 207 *et seq.*; Massachusetts General Laws Ch. 93A *et seq.*; Md. Com. Law Code § 13-101 *et seq.*; Mich. Stat. § 445.901 *et seq.*; Minn. Stat. § 8.31 *et seq.*; Miss. Code Ann. § 75-24-1 *et seq.*; Mo. Ann. Stat. § 407.010 *et seq.*; Mont. Code § 30-14-101 *et seq.*; Neb. Rev. Stat. § 59-1601 *et seq.*; Nev. Rev. Stat. § 598.0903 *et seq.*; N.H. Rev. Stat. § 358-A:1 *et seq.*; N.J. Rev. Stat. § 56:8-1 *et seq.*; N.M. Stat. § 57-12-1 et seq; N.Y. Gen. Bus. Law § 349 *et seq.*; N.C. Gen. Stat. §§ 75-1.1 *et seq.*; N.D. Cent. Code § 51-15-01 *et seq.*; Ohio Rev. Stat. § 1345.01 *et seq.*; Okla. Stat. 15 § 751 *et seq.*; Or. Rev. Stat. § 646.605 *et seq.*; 73 Pa. Stat. § 201-1 *et seq.*; R.I. Gen. Laws § 6-13.1-1 *et seq.*; S.C. Code Laws § 39-5-10 *et seq.*; S.D. Code Laws § 37-241 *et seq.*; Tenn. Code Ann. § 47-18-101 *et seq.*; Tex. Bus. & Com. Code § 17.41 *et seq.*; Utah Code § 13-11-1 *et seq.*; 9 Vt. Stat. § 2451 *et seq.*; Va. Code § 59.1-196 *et seq.*; Wash. Rev. Code § 19.86.010 *et seq.*; W. Va. Code § 46A-6-101 *et seq.*; Wis. Stat. § 100.18 *et seq.*; and Wyo. Stat. Ann. § 40-12-101 *et seq. See* Eighth Claim for Relief in Master Complaints. The Sprint Master Complaint asserts a claim for relief under the Kentucky consumer protection statute only.

[17] *See* Ninth Claim for Relief, MCI/Verizon Master Compl.; Fourteenth Claim for Relief, BellSouth Master Compl.; Ninth Claim for Relief, Sprint Master Compl.; Tenth Claim for Relief, Transworld Master Compl.; Twenty-Fourth Claim for Relief, Cingular Master Compl.

[18] *See* Fifteenth Claim for Relief, BellSouth Master Compl.; Tenth Claim for Relief, Sprint Master Compl.; Twenty-Fifth Claim for Relief, Cingular Master Compl.

[19] *See* BellSouth Master Compl., Eighth Claim for Relief.

[20] *See id.*, Tenth Claim for Relief.

[21] *See* Cingular Master Compl., Tenth Claim for Relief.

[22] *See id.*, Thirteenth Claim for Relief.

[23] *See id.*, Fourteenth Claim for Relief.

[24] *See id.*, Fifteenth Claim for Relief.

[25] *See id.*, Seventeenth Claim for Relief.

[26] *See id.*, Eighteenth and Nineteenth Claims for Relief.

While litigation of these state law claims, and the defenses thereto, will no doubt be controlled or impacted by the Court's rulings in *Hepting*, these claims have not yet been asserted in *Hepting*[30] or addressed by the Court. Because the Court's rulings on the state secrets issues should apply equally to Plaintiffs' state and federal claims, Plaintiffs respectfully suggest that the Court's rulings on the state secrets issues in connection with the OSC apply to Plaintiffs' state law claims as well.

However, Plaintiffs believe that litigation of the legal elements and defenses of their state law claims should be deferred for the time being, as (1) the declaratory relief, injunctive relief, and statutory damages available on Class Plaintiffs' federal statutory and constitutional claims may provide sufficient redress for their injuries; (2) the scope of discovery on the federal and state law claims appears to be the same; and (3) litigation of the elements and defenses particular to state law claims at this time might bog the case down in a complex and unnecessary battle over federal preemption and the elements of over 100 state statutes and the defenses thereto. To avoid premature and/or unnecessary litigation over these issues, Plaintiffs respectfully suggest that Defendants not be required to plead in response to Plaintiffs' state law claims, pending further order of the Court.[31]

---

[27] *See id.*, Twenty-First Claim for Relief.

[28] *Campbell v. AT&T Communications of California*, C-06-3596 VRW.

[29] *Riordan v. Verizon Communications, Inc.*, C-06-3574 VRW.

[30] As noted above, *Hepting* has been determined to be the lead case against the AT&T Defendants. AT&T Interim Class Counsel anticipate either amending or consolidating the multiple cases against AT&T when the *Hepting* appeal is complete, and will likely add some or all of the state law claims raised in the Master Complaints at that time.

[31] Plaintiffs cannot anticipate all of the circumstances which might make it appropriate for litigation of their state law claims to move forward, and so would oppose a stay pending resolution of their federal claims.

III. THE FACTUAL RECORD

The government has repeatedly acknowledged the similarity of the factual allegations made in *Hepting* and the instant cases. *See, e.g.,* Joint Case Management Conference Statement ("Joint CMC Stmt.," Dkt. No. 61-1) at 7:14-16 ("The transferred cases raise allegations similar to those raised in *Hepting* and *Terkel* concerning the interception of communications and the production of call record information"). Much of the material relied on by the Court in *Hepting* concerned plaintiffs' content claims. That information, and the conclusions drawn from it by the Court, are equally applicable here. The Court also had before it certain information concerning the call records program. But the Master Complaints, and additional information from members of Congress of which the Court may take judicial notice, go considerably further. This additional information, including on the record statements by three members of the Senate Select Committee on Intelligence who had been briefed on the call records program by the Executive branch, unequivocally confirm the existence of the call records program, and two of its participants — AT&T and MCI. The relevant factual material is summarized below.

A. Publicly Disclosed Information About the NSA Surveillance Program That Was Before The Court in *Hepting*

In *Hepting*, the Court catalogued the information that had been made public about "at least two different types of alleged NSA surveillance programs" (439 F. Supp. 2d at 986), all of which is included in the Master Complaints:[32]

- The confirmation by both the President and the Attorney General of the existence of the "terrorist surveillance program" first reported by the New York Times on December 16, 2005, the scope of the program, and the mechanism by which the program is authorized and reviewed.[33]

- The May 11, 2006 revelations by *USA Today* that BellSouth Corp., Verizon Communications, Inc and AT&T were providing telephone calling records of tens of millions of Americans to the NSA, which the NSA uses "to analyze calling patterns in an effort to detect terrorist activity."[34]

---

[32] *See* MCI/Verizon Master Compl., ¶¶ 138-41, 149-51, 153; BellSouth Master Compl., ¶¶ 38-41, 50-52, 55; Sprint Master Compl., ¶¶ 18-21, 30-32, 35; Transworld Master Compl., ¶¶ 21-24, 32-34, 36; Cingular Master Compl., ¶¶ 26-29, 38-40, 43. Out of an abundance of caution, Plaintiffs are submitting copies of the documents from which these allegations were drawn as exhibits to the Declaration of Barry Himmelstein and Request for Judicial Notice in Support of Class Plaintiffs' Response to Order to Show Cause Why Rulings on *Hepting* Motions to Dismiss Should Not Apply ("Himmelstein Decl.").

[33] *Hepting*, 439 F. Supp. 2d at 986-87. *See also* Himmelstein Decl., Exhs. A, B, and C.

- The release of a statement by the Attorney for Qwest Communications' former CEO, Joseph Nacchio, which detailed how he had been asked to participate in the call records program (thereby confirming its existence), but declined to do so because of the government's unwillingness to provide Qwest with legal process:

> In the Fall of 2001 * * * while Mr. Nacchio was Chairman and CEO of Qwest and was serving pursuant to the President's appointment as the Chairman of the National Security Telecommunications Advisory Committee, Qwest was approached to permit the Government access to the private telephone records of Qwest customers.
>
> Mr. Nacchio made inquiry as to whether a warrant or other legal process had been secured in support of that request. When he learned that no such authority had been granted and that there was a disinclination on the part of the authorities to use any legal process, including the Special Court which had been established to handle such matters, Mr. Nacchio concluded that these requests violated the privacy requirements of the Telecommications [sic] Act. Accordingly, Mr. Nacchio issued instructions to refuse to comply with these requests. These requests continued throughout Mr. Nacchio's tenure and until his departure in June of 2002.[35]

- The public statements made by defendants BellSouth and Verizon denying their involvement in the call records program.[36] The BellSouth statement read in relevant part:

> As a result of media reports that BellSouth provided massive amounts of customer calling information under a contract with the NSA, the Company conducted an internal review to determine the facts. Based on our review to date, we have confirmed no such contract exists and we have not provided bulk customer calling records to the NSA.[37]

Verizon stated, in relevant part:

> One of the most glaring and repeated falsehoods in the media reporting is the assertion that, in the aftermath of the 9/11 attacks, Verizon was approached by NSA and entered into an arrangement to provide the NSA with data from its customers' domestic calls.
>
> This is false. From the time of the 9/11 attacks *until just four*

---

[34] *Id.* at 988. *See also* Himmelstein Decl., Exh. K at 1.
[35] *Id.* *See also* Himmelstein Decl., Exh. N.
[36] *Id.* at 988.
[37] *Id.* *See also* Himmelstein Decl., Exh. Q.

> *months ago, Verizon had three major businesses-* its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of *these businesses*, or any call data from *those records*. None of *these companies*-wireless or wireline-provided customer records or call data.[38]

- Although not quoted by the Court in *Hepting,* Verizon's statement went on to say:

> Verizon cannot and will not confirm or deny whether it has any relationship to the classified NSA program. Verizon always stands ready, however, to help protect the country from terrorist attack. We owe this duty to our fellow citizens. We also have a duty, that we have always fulfilled, to protect the privacy of our customers. The two are not in conflict. When asked for help, we will always make sure that any assistance is authorized by law and that our customers' privacy is safeguarded.[39]

- Unlike defendants BellSouth and Verizon, neither AT&T nor the government has confirmed or denied the existence of a program of providing telephone calling records to the NSA.[40]

B. Statements By Members of Congress Who Have Been Briefed on the Call Records Program

While the Court in *Hepting* concluded that it did not have enough publicly available information either from the government or the carriers to permit discovery to go forward on the call records program, additional, authoritative information further confirming the existence of the call records program is now available. First, members of Congress who have been briefed extensively about the surveillance programs by the Administration have confirmed its existence. Among them are at least three members of the Senate Select Committee on Intelligence, all of whom have gone on the record confirming the existence of the records program.

Shortly after the May 11, 2006 *USA Today* report on the records program, the Chairman of the Senate Intelligence Committee, Kansas Senator Pat Roberts, was specifically asked about that program on the National Public Radio news program, "All Things Considered." In discussing the program, Senator Roberts explained how he and members of his Committee had detailed knowledge of the program:

---

[38] *Id*. at 988-89 (emphasis added).

[39] News Release, *Verizon Issues Statement on NSA Media Coverage* (May 16, 2006), available at http://newscenter.verizon.com/ proactive/newsroom/release.vtml?id=93450 (Himmelstein Decl., Exh. R). Verizon's statement bears striking resemblance to several AT&T statements relied upon by the Court in *Hepting*, 429 F. Supp. 2d at 992, indicating that, when asked, Verizon will provide assistance to the government if it believes the request to be lawful.

[40] *Hepting*, 439 F. Supp. 2d at 989.

> [Melissa] BLOCK: Let me clarify, because it seems we're talking about two different programs. One of which does involve monitoring. It involves domestic calls to numbers overseas back and forth. The other has to do with the collection of phone records, which did not involve monitoring.
>
> Regardless, I wanted to ask you about a comment from your colleague Republican Senator Arlen Specter, who made the point over the weekend that there has been no meaningful Congressional oversight of these programs. Do you agree?
>
> Senator ROBERTS: No, I don't. Arlen has not been read into the operational details of the program. I have ever since the inception of the program, along with Senator Rockefeller and along with our two counterparts in the House and along with the leadership. If you attend these briefings, and there have been many of them, and you ask tough questions and you get the answers that you want back, or if you don't, you go back and you ask another question and you make sure of it, I don't know what part of oversight that is not.
>
> Basically, that was expanded so that we had a seven member subcommittee. We've had, what, three or four hearings, numerous briefings. We've actually gone out and seen the program at work. We visited with the people who run it. I don't know of any program that is more scrutinized than this one, so we have had oversight. Senator Specter has not been read into the operational details and so I think that is his concern.
>
> BLOCK: You're saying that you are read into it. *I'm curious then if you're saying that you have had oversight directly of the program as has been reported, under which the NSA has collected millions of phone records of domestic calls.*
>
> Senator ROBERTS: Well, basically**,** *if you want to get into that, we're talking about business records.* We're not, you know, we're not listening to anybody. This isn't a situation where if I call you, you call me, or if I call home or whatever, that that conversation is being listened to.
>
> BLOCK: But those records are being kept and turned over to the government?
>
> Senator ROBERTS: I really can't comment on the details of the program. I can just tell you that basically what we have is a very highly minimized military capability to detect and deter and stop terrorist attacks and that's precisely what it does.[41]

---

[41] *Senate Intelligence Chair Readies For Hayden Hearings*, NPR All Things Considered, May 17, 2006 (Himmelstein Decl., Exh. T at 2) (emphasis added).

On May 16, 2006, CBS News reported that Senator "Roberts tells [CBS News correspondent Gloria] Borger that the NSA was looking at the phone calls collected during the surveillance, but he said not at the content, just at the pattern of phone calls."[42]

Similarly, the same day that *USA Today* ran its initial story about the call records program, Senator Kit Bond, another member of the same subcommittee of the Senate Intelligence Committee, also confirmed that he had been briefed on the existence of the call records program, this time on PBS' The News Hour with Jim Lehrer:

> JIM LEHRER: Senator Bond, how do you respond to that – you're a member – first of all, let me ask you directly. You're a member of the Senate Intelligence Committee. Did you know about this?
>
> SEN. KIT BOND, R-Mo.: Yes. I'm a member of the subcommittee of the Intelligence Committee that's been thoroughly briefed on this program and other programs.
>
> * * *
>
> Now, to move on to the points, number one, my colleague, Senator Leahy, is a good lawyer, and I believe that he knows, as any lawyer should know, that business records are not protected by the Fourth Amendment.
>
> The case of Smith v. Maryland in 1979, the U.S. Supreme Court said that the government could continue to use phone records, who called from where to where, at what time, for what length, for intelligence and criminal investigations without a warrant.
>
> This has been going on, and this has been gone on long before the president's program started. . . .
>
> JIM LEHRER: Excuse me, Senator Leahy, and let me just ask just one follow-up question to Senator Bond so we understand what this is about.
>
> What these are, are records. And nobody then -- now, these are -- but there are tens of millions of records that are in this database, right? And they say somebody, Billy Bob called Sammy Sue or whatever, and that's all it says, and then they go and try to match them with other people?
>
> SEN. KIT BOND: First, let me say that I'm not commenting on in any way any of the allegations made in the news story today. *I can tell you about the president's program.*
>
> *The president's program uses information collected from phone companies. The phone companies keep their records. They have a*

[42] *Congress To Be Briefed On NSA*, CBS News, May 16, 2006 (Himmelstein Decl., Exh. W), p. 1.

> *record. And it shows what telephone number called what other telephone number.*[43]

Former Senate Majority Leader William Frist, who, as part of the Senate leadership and as an *ex officio* member of the Senate Intelligence Committee, was briefed on the call records program, also confirmed the existence of the program to CNN's Wolf Blitzer:

> BLITZER: Let's talk about the surveillance program here in the United States since 9/11. USA Today reported a bombshell this week. Let me read to you from the article on Thursday.
>
> *"The National Security Agency has been secretly collecting the phone call records of tens of millions of Americans using data provided by AT&T, Verizon and BellSouth.* The NSA program reaches into homes and businesses across the nation by amassing information about the calls of ordinary Americans, most of whom aren't suspected of any crime. With access to records of billions of domestic calls, the NSA has gained a secret window into the communications habits of millions of Americans."
>
> *Are you comfortable with this program?*
>
> FRIST**:** *Absolutely. Absolutely. I am one of the people who are briefed…*
>
> BLITZER: You've known about this for years.
>
> FRIST: *I've known about the program. I am absolutely convinced that you, your family, our families are safer because of this particular program.*[44]

The substance of each of these interviews is alleged in each of the Master Complaints.[45]

In a May 16, 2006 White House Press Briefing, in response to a question whether the records program "has been fully briefed to members in the United States Congress," White House Press Secretary Tony Snow responded that "all intelligence matters conducted by the National Security Agency — and we've said this many times — have been fully briefed to a handful of members of the Senate Intelligence and House Intelligence Committees and to the leadership."[46]

---

[43] PBS Online NewsHour, *NSA Wire Tapping Program Revealed*, May 11, 2006 (Himmelstein Decl., Exh. L at 4-5) (emphasis added).

[44] CNN Late Edition with Wolf Blitzer, May 14, 2006 (Himmelstein Decl., Exh. P at 13) (emphasis added).

[45] *See* MCI/Verizon Master Compl., ¶¶ 154-56; BellSouth Master Compl., ¶¶ 56-58; Sprint Master Compl., ¶¶ 36-38; Transworld Master Compl., ¶¶ 37-38; Cingular Master Compl., ¶¶ 44-46.

In a May 17, 2006 letter to then Speaker of the House of Representatives the Hon. Dennis J. Hastert, the Director of National Intelligence, John D. Negroponte, provided a list "of the dates, locations, and names of members of Congress who attended briefings on the Terrorist Surveillance Program," expressly stating that "this information can be made available in an unclassified format," and that "[t]he briefings typically occurred at the White House prior to December 17, 2005. After December 17, the briefings occurred at the Capitol, NSA, or the White House." Himmelstein Decl., Exh. Y. Consistent with Senator Roberts' interview, the attached list confirms that the Senator was briefed on the program on ten such occasions over a period of more than three years. *See id.* (29-Jan-03, 17-Jul-03, 0-Mar-04, 3-Feb-05, 14-Sep-05, 11-Jan-06, 20-Jan-06, 11-Feb-06, 9-Mar-06, 13-Mar-06). The same list confirms that Senator Bond was briefed on the program twice in March 2006, and that Senator Frist was briefed on the program in March 2004 and January 2006. *Id.* As noted by Senator Bond in his interview, Senator Spector's name does not appear on the list. *Id.*

The same day, at a White House Press Briefing, Mr. Snow explained that while such briefings had previously been limited, the full membership of the Intelligence Committees would be briefed on the "the entire scope of NSA surveillance," and not merely the contents program that the President had publicly acknowledged:

> First: Who is doing the briefings in the National Security Agency? That is already out and about now, but it's General Keith Alexander; the NSA Director is doing the briefings on the Hill.
>
> * * *
>
> Q Okay, but the briefing is the full Senate --
>
> MR. SNOW: The full Senate Intelligence Committee and the full House Intelligence Committee -- the full Senate [Intelligence Committee] today.
>
> Q This seems to be a bit of a departure from what we were previously led to believe. What's behind "the more, the merrier"?
>
> MR. SNOW: What's behind -- how about "the more, the better

---

[46] *Press Briefing by Tony Snow*, The White House, Office of the Press Secretary, May 16, 2006 (Himmelstein Decl., Exh. X) at 1.

> informed"? As Senator Roberts said earlier today, he thought it was an uncomfortable situation in which you would have seven members fully briefed on the program as they're getting ready to do confirmation hearings, and eight members not briefed. There was a strong sense that everybody needed to be read into the program to do what they needed, in his opinion, to do to have a full and appropriate confirmation hearing for General Hayden. And we agreed with him.
>
> * * *
>
> Q Can I go back to the NSA briefings that are going on May 17, 2006? Is the briefing going to be limited to the program that the President has publicly acknowledged? Or is it going to be the entire scope of NSA surveillance? Will the people who are briefed get the full picture of what is going on?
>
> MR. SNOW: Permit me to turn to my trustworthy assistants.
>
> MS. PERINO: Full terrorist surveillance program.
>
> MR. SNOW: Full terrorist surveillance program.

Press Briefing by Tony Snow, The White House, Office of the Press Secretary, May 17, 2006 (Himmelstein Decl., Exh. Z), at 1-2, 8.

Following these briefings, on June 30, 2006, *USA Today* reported that:

> Nineteen lawmakers who had been briefed on the program verified that the NSA has built a database that includes records of Americans' domestic phone calls. The program collected records of the numbers dialed and the length of calls, sources have said, but did not involve listening to the calls or recording their content.
>
> • Five members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program.
>
> * * *
>
> • [Four lawmakers] said MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the government.

Himmelstein Decl., Exh. V at 1-2. *See* BellSouth Master Compl., ¶ 60; Sprint Master Compl., ¶ 40; Transworld Master Compl., ¶ 40; Cingular Master Compl., ¶ 48.

C. Additional Public Disclosures Not Discussed in *Hepting*

The Master Complaints contain further public disclosures regarding the existence and operation of the government's surveillance programs, including the call records program. These disclosures provide added detail about the programs:

On December 24, 2005, *The New York Times* reported in an article entitled, "Spy Agency Mined Vast Data Trove, Officials Report"[47] that:

> The National Security Agency has traced and analyzed large volumes of telephone and Internet communications flowing into and out of the United States as part of the eavesdropping program that President Bush approved after the Sept. 11, 2001 attacks to hunt for evidence of terrorist activity, according to current and former government officials. The volume of information harvested from telecommunication data and voice networks, without court-approved warrants, is much larger than the White House has acknowledged, the officials said. It was collected by tapping directly into some of the American telecommunication system's main arteries, they said.
>
> The officials said that as part of the program, "the N.S.A. has gained the cooperation of American telecommunications companies to obtain backdoor access to streams of domestic and international communications," and that the program is a "large data-mining operation," in which N.S.A. technicians have combed through large volumes of phone and Internet traffic in search of patterns that might point to terrorism suspects. In addition, the article reports, "[s]everal officials said that after President Bush's order authorizing the N.S.A. program, senior government officials arranged with officials of some of the nation's largest telecommunications companies to gain access to switches that act as gateways at the borders between the United States' communication networks and international networks."

In a January 3, 2006 article entitled, "Tinker, Tailor, Miner, Spy" (available at http://www.slate.com/toolbar.aspx?action=print&id=2133564),[48] Slate.com reported:

> The agency [the NSA] used to search the transmissions it monitors for key words, such as names and phone numbers, which are supplied by other intelligence agencies that want to track certain individuals. But now the NSA appears to be vacuuming up all data, generally without a particular phone line, name, or e-mail address as a target. Reportedly, the agency is analyzing the length of a call, the time it was placed, and the origin and destination of electronic transmissions.

In a January 17, 2006 article, "Spy Agency Data After Sept. 11 Led F.B.I. to Dead Ends,"[49] *The New York Times* stated that officials who were briefed on the N.S.A. program said that:

---

[47] Himmelstein Decl., Exh. D at 1-2.

[48] Himmelstein Decl., Exh. E at 2.

[49] Himmelstein Decl., Exh. F at 2-3.

> the agency collected much of the data passed on to the F.B.I. as tips by tracing phone numbers in the United States called by suspects overseas, and then by following the domestic numbers to other numbers called. In other cases, lists of phone numbers appeared to result from the agency's computerized scanning of communications coming into and going out of the country for names and keywords that might be of interest.

A January 20, 2006 article in the *National Journal*, "NSA Spy Program Hinges On State-of-the-Art Technology,"[50] reported that:

> Officials with some of the nation's leading telecommunications companies have said they gave the NSA access to their switches, the hubs through which enormous volumes of phone and e-mail traffic pass every day, to aid the agency's effort to determine exactly whom suspected Qaeda figures were calling in the United States and abroad and who else was calling those numbers. The NSA used the intercepts to construct webs of potentially interrelated persons.

In a January 21, 2006 article in *Bloomberg News* entitled "Lawmaker Queries Microsoft, Other Companies on NSA Wiretaps,"[51] Daniel Berninger, a senior analyst at Tier 1 Research in Plymouth, Minnesota, said,

> in the past, the NSA has gotten permission from phone companies to gain access to so-called switches, high-powered computers into which phone traffic flows and is redirected, at 600 locations across the nation. . . . From these corporate relationships, the NSA can get the content of calls and records on their date, time, length, origin and destination.

On February 5, 2006, an article appearing in the *Washington Post* entitled "Surveillance Net Yields Few Suspects"[52] stated that officials said "[s]urveillance takes place in several stages . . . the earliest by machine. Computer-controlled systems collect and sift basic information about hundreds of thousands of faxes, e-mails and telephone calls into and out of the United States before selecting the ones for scrutiny by human eyes and hears. Successive stages of filtering grow more intrusive as artificial intelligence systems rank voice and data traffic in order of likeliest interest to human analysts." The article continues, "[f]or years, including in public testimony by Hayden, the agency [the NSA] has acknowledged use of automated equipment to analyze the contents and guide analysts to the most important ones. According to one knowledgeable source, the warrantless program also uses those methods. That is significant . . . because this kind of filtering intrudes into content, and machines 'listen' to more Americans than

[50] Himmelstein Decl., Exh. G at 2.

[51] Himmelstein Decl., Exh. H at 1.

[52] Himmelstein Decl., Exh. I at 1, 5.

> humans do."
>
> On February 6, 2006, in an article entitled "Telecoms let NSA spy on calls,"[53] the nationwide newspaper *USA Today* reported that "[t]he National Security Agency has secured the cooperation of large telecommunications companies, including AT&T, MCI and Sprint, in its efforts to eavesdrop without warrants on international calls by suspected terrorists, according to seven telecommunications executives." The article acknowledged that The *New York Times* had previously reported that the telecommunications companies had been cooperating with the government but had not revealed the names of the companies involved. In addition, it stated that long-distance carriers AT&T, MCI, and Sprint "all own 'gateway' switches capable of routing calls to points around the globe," and that "[t]elecommunications executives say MCI, AT&T, and Sprint grant the access to their systems without warrants or court orders. Instead, they are cooperating on the basis of oral requests from senior government officials."
>
> * * *
>
> On May 29, 2006, Seymour Hersh reported in *The New Yorker* in an article entitled "Listening In"[54] that a security consultant working with a major telecommunications carrier "told me that his client set up a top-secret high-speed circuit between its main computer complex and Quantico, Virginia, the site of a government-intelligence computer center. This link provided direct access to the carrier's network core – the critical area of its system, where all its data are stored. 'What the companies are doing is worse than turning over records,' the consultant said. 'They're providing total access to all the data.'"

MCI/Verizon Master Compl., ¶¶ 142-48, 157. *See also* BellSouth Master Compl., ¶¶ 42-49, 59; Sprint Master Compl., ¶¶ 22-29, 39; Transworld Master Compl., ¶¶ 25-31, 39; Cingular Master Compl., ¶¶ 30-37, 47.

IV. WITH ONE EXCEPTION, THE COURT'S RULINGS ON THE STATE SECRETS ISSUES IN *HEPTING* ARE EQUALLY APPLICABLE HERE

In *Hepting*, the United States moved to intervene in order to assert the state secrets privilege, and moved for dismissal or summary judgment based on the privilege. While the government has not as yet intervened in any of the cases made part of this MDL proceeding other than *Hepting* and *Terkel*,[55] it has stated that if the other cases are not stayed, "the Government expects to assert the state secrets privilege in all the cases currently transferred." Joint CMC Stmt., at 26:15-16. To avoid unnecessary litigation over the propriety of intervention, Plaintiffs are willing to stipulate to intervention by the government in each of the cases for the limited purpose of asserting the state secrets privilege.

---

[53] Himmelstein Decl., Exh. J at 1-2.

[54] Himmelstein Decl., Exh. U at 1.

[55] *Terkel v. AT&T Corp.*, 441 F. Supp. 2d 899 (N.D. Ill. 2006) ("*Terkel*") (N.D. Ill. Case No. 06-C-2837).

In *Hepting*, the Court agreed that "that the government has satisfied the three threshold requirements for properly asserting the state secrets privilege: (1) the head of the relevant department, Director of National Intelligence John D Negroponte (2) has lodged a formal claim of privilege (3) after personally considering the matter. Moreover, the Director of the NSA, Lieutenant General Keith B Alexander, has filed a declaration supporting Director Negroponte's assertion of the privilege." *Id.* at 993 (citations omitted). While the government may choose not to re-submit these declarations in response to the Court's order to show cause, the unclassified versions of the declarations remain part of the record in this multidistrict litigation proceeding, and the government has expressly confirmed that "[t]his MDL proceeding presents the same state secrets privilege issues that previously have been raised by the United States in the *Hepting* and *Terkel* actions." Joint CMC Stmt. at 15:10-12. Indeed, the government has *complained* that it would be a "burdensome undertaking" to require it to relitigate the state secrets issues (*id.* at 22:19). As with intervention, Plaintiffs are willing to spare the government this effort, and will stipulate that both the public and non-public versions of the declarations submitted by the government in connection with the motions to dismiss in *Hepting* may be considered by the Court in ruling on its order to show cause.[56]

In *Hepting*, the government argued that the state secrets privilege required dismissal of the action or granting summary judgment for AT&T on numerous grounds, including that:

> (1) the very subject matter of this case is a state secret; (2) plaintiffs cannot make a *prima facie* case for their claims without classified evidence and (3) the privilege effectively deprives AT&T of information necessary to raise valid defenses.

Id. at 985. The Court also considered whether the *Hepting* claims were barred by the categorical

[56] By so stipulating, Plaintiffs do not waive the right to seek to have the declarations or portions thereof unsealed.

Totten/Tenet bar. *See Totten v. United States*, 92 U.S. 105 (1876); *Tenet v. Doe*, 544 U.S. 1 (2005). Each of these arguments is addressed separately below.[57]

A. The Categorical *Totten/Tenet* Bar Does Not Apply

As the Supreme Court recently observed, the "categorical *Totten* bar" is limited to "the distinct class of cases that depend upon clandestine spy relationships." *Tenet*, 544 U.S. at 9. As this Court observed in *Hepting*, in distinguishing these cases:

> *Totten* and *Tenet* are not on point to the extent they hold that former spies cannot enforce agreements with the government because the parties implicitly agreed that such suits would be barred. The implicit notion in *Totten* was one of equitable estoppel: one who agrees to conduct covert operations impliedly agrees not to reveal the agreement even if the agreement is breached. But AT&T, the alleged spy, is not the plaintiff here. In this case, plaintiffs made no agreement with the government and are not bound by any implied covenant of secrecy.
>
> * * *
>
> The court's conclusion here follows the path set in *Halkin v. Helms* and *Ellsberg v. Mitchell*, the two cases most factually similar to the present. The *Halkin* and *Ellsberg* courts did not preclude suit because of a *Totten*-based implied covenant of silence. . . . [T]he court sees no reason to apply the *Totten* bar here.

Id. at 991, 993. *Accord Terkel*, 441 F. Supp. 2d at 907 (distinguishing *Totten* and *Tenet* on same grounds).

The Court's reasoning is equally applicable to Defendants. Plaintiffs, and the members of the classes they seek to represent, are the objects of the alleged espionage, not its agents. They "made no agreement with the government and are not bound by any implied covenant of secrecy." 439 F. Supp. 2d at 991. On the contrary, Plaintiffs were assured by Defendants via their respective privacy policies that the confidentiality of Plaintiffs' communications and records would be maintained inviolate, except as required by law.[58] If

---

[57] As set forth above, Plaintiffs are willing to defer litigation on the elements of their state law claims. However, the Court's rulings in *Hepting* on the state secrets issue and federal statutory privileges are equally applicable to Plaintiffs' state law claims, which are based on common factual allegations. Accordingly, the Court's rulings on these issues should apply to the state law claims asserted in the Master Complaints, *Campbell*, and *Riordan*.

[58] *See* MCI/Verizon Master Compl., ¶¶ 179-81, 268, 274; BellSouth Master Compl., ¶¶ 203, 208, 213; Sprint Master Compl., ¶¶ 140, 144, 149; Transworld Master Compl., ¶¶ 174, 179; Cingular Master Compl., ¶¶ 211, 229-30, 237, 265, 269, 274.

Plaintiffs had any expectations arising out of their contractual relationships with their carriers, it was that their carriers would abide by these policies and obey the law, not engineer their wholesale violation. Accordingly, the categorical *Totten/Tenet* bar does not apply.

B. The Very Subject Matter of the Actions is Not a State Secret

As the Court noted, "no case dismissed because its 'very subject matter' was a state secret involved ongoing, widespread violations of individual constitutional rights, as plaintiffs allege here." *Id.* at 993. Plaintiffs hasten to add that they are unaware of any case dismissed on state secret grounds which involved anything remotely approaching the widespread violations of federal privacy statutes alleged here, which define the permissible bounds of behavior for telecommunications carriers. By contrast, the Court noted that "most cases in which the 'very subject matter' was a state secret involved classified details about either a highly technical invention or a covert espionage relationship." *Id.* (citations omitted). As in *Hepting*, these cases involve neither, and "focus[] only on whether [Defendants] intercepted and disclosed communications or communications records to the government." *Id.* at 994. As the Court held in *Hepting*, given the "significant amounts of information about the government's monitoring of communications content" already in the public record (*see* Part III.A., *supra*), "the very subject matter of this action is hardly a secret," and the actions should not be dismissed on that ground. *Id.*[59]

C. Dismissal on Evidentiary Grounds Would Be Premature

In *Hepting*, the Court held that it would be "premature" to "decide at this time whether this case should be dismissed on the ground that the government's state secrets assertion will preclude evidence necessary for plaintiffs to establish a *prima facie* case or for AT&T to raise a valid defense to the claims." 439 F. Supp. 2d at 994. In so holding, the Court noted its subsequent finding that "Plaintiffs appear to be entitled to at least some discovery," and followed the approach taken in other cases of "allow[ing] them to proceed to discovery sufficiently to assess the state secrets privilege in light of the facts." *Id.* Just as "[t]he government has not shown why that should not be the course of this litigation [*Hepting*]" (*id.*), there is no reason to depart from the Court's holding here.

---

[59] *See also*, *Terkel*, 441 F. Supp. 2d at 908 (finding that "the very subject matter of this lawsuit is not necessarily a state secret").

D. The Existence or Non-Existence of a Certification Is Not a State Secret

In *Hepting*, the government argued that "the issue whether AT&T received a certification authorizing its assistance to the government is a state secret." *Id.* at 995. The Court held that, given that the government had admitted monitoring international-domestic communications where it suspects that one party to the communication is affiliated with al Qaeda:

> revealing whether AT&T has received a certification to assist in monitoring communication content should not reveal any new information that would assist a terrorist and adversely affect national security. And if the government has not been truthful, the state secrets privilege should not serve as a shield for its false public statements.

Id. at 996. The disclosures found dispositive by the Court are not carrier-specific, and apply equally to all Defendants. Accordingly, the court's conclusion "that the state secrets privilege will not prevent AT&T from asserting a certification-based defense, as appropriate, regarding allegations that it assisted the government in monitoring communication content," is equally applicable here.[60]

Indeed, the government's recent submission (Dkt. 127) stating that "any electronic surveillance that was occurring as part of the Terrorist Surveillance Program (TSP) will now be conducted subject to the approval of the Foreign Intelligence Surveillance Court," eliminates any secrecy concerning the existence or non-existence of a certification, and makes it appropriate for the Court to proceed under 50 U.S.C. § 1806(f), which requires that the Court "shall, notwithstanding any other law, . . . review in camera and *ex parte* the application, order, and such other materials relating to the surveillance as may be necessary to determine whether the surveillance of the aggrieved person was lawfully authorized and conducted."

E. The Statutory Privileges Do Not Warrant Dismissal

Finally, in *Hepting*, the government argued that dismissal was required by two "statutory privileges," 50 U.S.C. § 402 *note*, §6, which protects "information with respect to the

[60] The issue of whether the existence of the records program remains a genuine "secret" is addressed in Part V, *infra*.

activities" of the NSA, and 50 U.S.C. § 403-1(i)(1), which requires the Director of National Intelligence to "protect intelligence sources and methods from unauthorized disclosure." *Id.* at 998. The Court rejected this argument, because "[n]either of these provisions by their terms requires the court to dismiss this action and it would be premature for the court to do so at this time." *Id.*[61] As the Court's holding is based on its interpretation of these statutes, not on facts unique to AT&T, the Court's holding is equally applicable here.

V. ADDITIONAL INFORMATION CONFIRMS THAT THE RECORDS PROGRAM IS NOT A SECRET

A. The Court's Ruling in *Hepting*

In determining whether the existence of the records program is a secret for purposes of the state secrets privilege, the Court noted that it "may rely upon reliable public evidence that might otherwise be inadmissible at trial because it does not comply with the technical requirements of the rules of evidence." 439 F. Supp. 2d at 991 (citing Fed. R. Evid. 104(a)). The Court reiterated that it would consider only "publicly reported information that possesses substantial indicia of reliability." *Id.* at 990. *Accord Terkel*, 441 F. Supp. 2d at 913 ("the focus should be on information that bears persuasive indication of reliability"). Applying this standard, the Court declined to "rely on media reports about the alleged NSA programs because their reliability is unclear," in light of conflicting reports regarding the involvement of Verizon and BellSouth in the records program. *Hepting*, 439 F. Supp. 2d at 991. The Court also declined to consider the Klein declaration in making its determination because "the inferences Klein draws have been disputed," and expressed concern that considering it "would invite attempts to undermine the privilege by mere assertions of knowledge by an interested party." *Id.*

[61] In *Terkel*, the Court expressed concern that if "section 6 is taken to its to its logical conclusion, it would allow the federal government to conceal information regarding blatantly illegal or unconstitutional activities simply by assigning these activities to the NSA or claiming they implicated information about the NSA's functions," and was "hard-pressed to read section 6 as essentially trumping every other Congressional enactment and Constitutional provision." 441 F. Supp. 2d at 905. Plaintiffs concur wholeheartedly with this wise judicial pronouncement. With respect to § 403-1(i)(1), the Court observed that "the plaintiffs have sued only AT&T and are seeking discovery only from that entity, not the Director of National Intelligence, the NSA, or any governmental agency. Under these circumstances, section [403-1(i)(1)] does not by itself bar prosecution of this case." *Id.* at 906.

at 990.[62]

Having eliminated the only other proffered sources of information, in making its determination, the Court considered "only public admissions or denials by the government, AT&T and other telecommunications companies, which are the parties indisputably situated to disclose whether and to what extent the alleged programs exist." *Id.*

Considering this limited set of information, the Court concluded that:

> despite many public reports on the matter, the government has neither confirmed nor denied whether it monitors communication records and has never publicly disclosed whether the NSA program reported by *USA Today* on May 11, 2006, actually exists. Although BellSouth, Verizon and Qwest have denied participating in this program, AT&T has neither confirmed nor denied its involvement. Hence, unlike the program monitoring communication content, the general contours and even the existence of the alleged communication records program remain unclear.

Id. at 997. However, the Court stressed that:

> While this case has been pending, the government and telecommunications companies have made substantial public disclosures on the alleged NSA programs. It is conceivable that these entities might disclose, either deliberately or accidentally, other pertinent information about the communication records program as this litigation proceeds. The court recognizes such disclosures might make this program's existence or non-existence no longer a secret. Accordingly, while the court presently declines to permit any discovery regarding the alleged communication records program, if appropriate, plaintiffs can request that the court revisit this issue in the future.

Id. at 997-98. The additional disclosures highlighted below fully warrant such revisitation.

B. The Existence of The Records Program Has Been Acknowledged by Nineteen Members of Congress Briefed on the Program by the NSA

While the May 11, 2006 *USA Today* story reporting the existence of the records program may have contained inaccuracies regarding the participants in the program, rendering its "reliability unclear," those inaccuracies have been corrected. As a result of the discussions, briefings, and disclosures generated by that article, what emerges is a coherent and consistent story bearing "substantial indicia of reliability." These disclosures leave no *reasonable* doubt that the records program exists, and that at a minimum, AT&T and Verizon's recently-acquired subsidiary, MCI, gave the NSA access to customer call records.

---

[62] Plaintiffs do not concede that Mr. Klein is an "interested party," or that the inferences drawn by the *Hepting* plaintiffs can reasonably be disputed, but as the Klein declaration is not directly at issue with respect to Defendants other than AT&T, Plaintiffs need not take issue with either point here.

Within days following publication of the May 11 story, which reported that Qwest Communications had refused to participate in the program, the former CEO of Qwest — a person "indisputably situated to disclose whether and to what extent the alleged programs exist" — issued a statement publicly confirming that he was repeatedly requested "to permit the Government access to the private telephone records of Qwest customers" without "a warrant or other legal process," but refused to comply because he "concluded that these requests violated the privacy requirements of the Telecommications [sic] Act." Himmelstein Decl., Exh. N.

Within a week following publication of the May 11 story, the Chairman of the Senate Select Committee on Intelligence, another of its members, and the Senate Majority Leader were interviewed concerning the story on NPR, PBS, and CNN, respectively, confirmed that they had been extensively briefed on the records program, establishing their knowledge; and confirmed its existence, although they declined to discuss its details. The Director of National Intelligence confirmed publicly and in writing that each of these Senators had been briefed repeatedly on the NSA's Terrorist Surveillance Program, and that such briefings had taken place at the White House, at the Capitol, and at the itself NSA, as Senator Roberts had described. *See* Part III.B., *supra*. *Compare Terkel*, 441 F. Supp. 2d at 914 (complaining that there was no way for the Court to determine whether the cited media reports were "based on information from persons who would have reliable knowledge about the existence or non-existence of the activity alleged").

Significantly, the public statements of Senators Bond and Roberts were not before the Courts in *Hepting* or *Terkel*. The fact that these Senators oversaw the program from The Capitol rather than The White House makes them no less statements by informed and credible government officials possessing "substantial indicia of reliability." *See Jabara v. Kelley*, 75 F.R.D. 475, 493 (E.D. Mich. 1977) (in view of report of Senate Select Committee on Intelligence disclosing name of federal agency "that has admittedly intercepted plaintiff's personal communications without prior court approval," it "would be a farce to conclude that the name of this other federal agency remains a military or state secret"). Considered in conjunction with additional published reports confirming the existence of the records program, the public status of the program can no longer reasonably be disputed.

Beginning on May 17, 2006, the Director of the NSA, Lt. General Keith B. Alexander, briefed the full membership of the Intelligence Committees on the "full" scope of NSA surveillance activities. Himmelstein Decl., Exh. Z, at 1-2, 8. Following these briefings, on June 30, 2006, with its journalistic integrity under attack by Verizon and BellSouth, who had denied participation in the records program, *USA Today* "set the record straight" in an article entitled "Lawmakers: NSA database incomplete" (the "June 30 article").[63] In a sidebar, "A Note To Our Readers," the paper acknowledged the controversy, explaining that:

> USA TODAY continued to pursue details of the database, speaking with dozens of sources in the telecommunications, intelligence and legislative communities, including interviews with members of Congress who have been briefed by senior intelligence officials on the domestic calls program.
>
> In the adjoining article, USA TODAY reports that five members of the congressional intelligence committees said they had been told in secret briefings that BellSouth did not turn over call records to the NSA, three lawmakers said they had been told that Verizon had not participated in the NSA database, and four said that Verizon's subsidiary MCI did turn over records to the NSA.

Himmelstein Decl., Exh. V at 1-2. The article also reported that ***nineteen*** members of the Senate and House Intelligence Committees who had been briefed on the records program confirmed its existence:

> Members of the House and Senate intelligence committees confirm that the National Security Agency has compiled a massive database of domestic phone call records. But some lawmakers also say that cooperation by the nation's telecommunication companies was not as extensive as first reported by USA TODAY on May 11.
>
> Several lawmakers, briefed in secret by intelligence officials about the program after the story was published, described a call records

[63] The *Hepting* plaintiffs filed their opposition to the government's motion to dismiss on June 8, 2006 (*see Hepting* Dkt. No. 181), three weeks before publication of the June 30 article, and the motion was argued on June 23, 2006, one week before publication of the article. While the *Hepting* plaintiffs moved to supplement the record with the article (Dkt. No. 299), that motion was never ruled upon, and the sole reference to the article in *Hepting* is the statement that "BellSouth and Verizon's denials have been at least somewhat substantiated in later reports." 439 F. Supp. 2d at 989.

database that is enormous but incomplete. Most asked that they not be identified by name, and many offered only limited responses to questions, citing national security concerns.

In the May 11 article that revealed the database, USA TODAY reported that its sources said AT&T, BellSouth and Verizon had agreed to provide the NSA with call records.

AT&T, which is the nation's largest telecommunications company, providing service to tens of millions of Americans, hasn't confirmed or denied its participation with the database. BellSouth and Verizon have denied that they contracted with the NSA to turn over phone records. On May 12, an attorney for former Qwest CEO Joseph Nacchio confirmed the USA TODAY report that Qwest had declined to participate in the NSA program.

Most members of the intelligence committees wouldn't discuss which companies cooperated with the NSA. However, several did offer more information about the program's breadth and scope, confirming some elements of USA TODAY's report and contradicting others:

• *Nineteen lawmakers who had been briefed on the program verified that the NSA has built a database that includes records of Americans' domestic phone calls. The program collected records of the numbers dialed and the length of calls, sources have said, but did not involve listening to the calls or recording their content.*

• *Five members of the intelligence committees said they were told by senior intelligence officials that AT&T participated in the NSA domestic calls program.*

* * *

• *Five members of the intelligence committees said they were told that BellSouth did not turn over domestic call records to the NSA.*

* * *

• *Three lawmakers said that they had been told that Verizon did not turn over call records to the NSA. However, those three and another lawmaker said MCI, the long-distance carrier that Verizon acquired in January, did provide call records to the government.*

Himmelstein Decl., Exh. V at 1-2 (emphasis added). Plaintiffs respectfully submit that confirmation by nineteen members of Congress briefed on the program by the NSA, reported by a reputable national newspaper that had an unusually strong interest in ensuring the accuracy of its reporting, bears "substantial indicia of reliability," even if the members are not identified by name, especially when considered in conjunction with "on-the-record" confirmations by three members of the Senate Intelligence Committee. The Nacchio statement buttresses this conclusion even further.

In *Hepting*, the Court declined to "estimate the risk tolerances of terrorists in making their communications and hence eschew[ed] the attempt to weigh the value of the information." 439 F. Supp. 2d at 990. Plaintiffs respectfully submit that in determining whether the existence of the records program, and the identity of the participating carriers, remains a "secret" for purposes of the state secrets privilege, the Court must assume that potential terrorists possess at least a modicum of common sense. Common sense requires potential terrorists to assume that the records program exists, and that AT&T and MCI have provided their customers' call detail records to the NSA. Accordingly, the program, and the participation of these carriers, is no longer a "secret," and Plaintiffs should be permitted discovery on their records claims.[64]

C. Verizon Has Tacitly Admitted That MCI Participated in the Records Program

Verizon's purported "denials," like BellSouth's, are fully consistent with the June 30 article. Verizon's carefully worded, May 16, 2006 "denial" bears repeating:

> From the time of the 9/11 attacks *until just four months ago, Verizon had three major businesses*-its wireline phone business, its wireless company and its directory publishing business. It also had its own Internet Service Provider and long-distance businesses. Contrary to the media reports, Verizon was not asked by NSA to provide, nor did Verizon provide, customer phone records from any of *these businesses*, or any call data from *those records*. None of *these companies*-wireless or wireline-provided customer records or call data.[65]

On May 16, 2006, *USA Today* reported that:

> Verizon's [May 16, 2006] statement does not mention MCI, the long-distance carrier the company bought in January. Before the sale, Verizon sold long-distance under its own brand. *Asked to elaborate on what role MCI had, or is having, in the NSA program, spokesman Peter Thonis said the statement was about Verizon, not MCI.*

MCI/Verizon Master Compl., ¶ 162; Himmelstein Decl., Exh. S at 2 (emphasis added). Taken together, these two statements — vehemently denying Verizon's own participation in the program, but *refusing* to deny the participation of its newly-acquired subsidiary, MCI — amount to a tacit admission that MCI did in fact participate in the program. *Cf. Hepting*, 439 F. Supp. 2d at 997-98 ("It is conceivable that [the telecommunications companies] might disclose, *either deliberately or accidentally*, other pertinent information about the communication records program" that might make the program's "existence or non-existence no longer a secret") (emphasis added). This inescapable conclusion is reinforced by another press release issued by Verizon the day after the May 11 story was published, entitled "Verizon Issues Statement on NSA and Privacy Protection":

---

[64] If the Court agrees that the additional information justifies discovery concerning the records claims against the other carriers, discovery concerning those claims against AT&T should be permitted as well.

[65] *Id.* at 988-89 (emphasis added).

> Verizon will provide customer information to a government agency only where authorized by law for appropriately-defined and focused purposes. . . . Verizon does not, and will not, provide any government agency unfettered access to our customer records or provide information to the government under circumstances that would allow a fishing expedition.
>
> In January 2006, Verizon acquired MCI, and *we are ensuring that Verizon's policies are implemented at that entity and that all its activities fully comply with law*.

MCI/Verizon Master Compl., ¶ 160; Himmelstein Decl., Exh. M (emphasis added). Read in conjunction with Verizon's May 16 statements, the clear implication of this dichotomous statement is that while *Verizon* did not provide the government with access to its customers' records, the same could not be said for MCI.

D. Discovery Concerning the Existence of Any Certifications Concerning the Records Program Received by Verizon and/or BellSouth Must Be Permitted

The fact that Verizon and BellSouth have issued denials concerning the call records program is significant for another reason. In *Hepting*, the Court noted that "[i]mportantly, the public denials by these telecommunications companies undercut the government and AT&T's contention that revealing AT&T's involvement or lack thereof in the [records] program would disclose a state secret." *Hepting*, 439 F. Supp.2d at 997. The Court's observation is even more apt here. Given that Verizon and BellSouth have voluntarily issued public denials via press release, it would be anomalous to hold that Plaintiffs are precluded from requiring these defendants to respond under oath to carefully tailored requests for admissions and interrogatories concerning the accuracy of their statements. As the Court held with respect to the government's admissions concerning the content program:

> Based on these public disclosures, the court cannot conclude that the existence of a certification regarding the "communication content" program is a state secret. If the government's public disclosures have been truthful, revealing whether AT&T has received a certification to assist in monitoring communication content should not reveal any new information that would assist a terrorist and adversely affect national security. And if the government has not been truthful, the state secrets privilege should not serve as a shield for its false public statements. In short, the government has opened the door for judicial inquiry by publicly confirming and denying material information about its monitoring of communication content.

Id. at 996. Consistent with this holding, discovery concerning the existence of any certifications concerning the records program received by Verizon and/or BellSouth must be permitted.

E. The Wholesale Violation of Federal Privacy Laws Cannot Be a "State Secret"

Finally, Plaintiffs join in the *Hepting* plaintiffs' argument that "Congress, through various statutes, has limited the state secrets privilege in the context of electronic surveillance and has abrogated the privilege regarding the existence of a government certification." 439 F. Supp. 2d at 998. Congress has enacted, and the President has signed into law, numerous statutes whose sole purpose is to *prevent* the government from intruding on the privacy of its citizens. Plaintiffs respectfully submit that the wholesale violation of these laws cannot be allowed to continue merely because the violations have occurred in secret. If it is a secret, it is not a secret that the law countenances be *kept*; it is a secret that must *come out*, or the rights conferred by these statutes — and the Fourth Amendment — become meaningless.

In *Hepting*, the Court "decline[d] to address these issues presently, particularly because the issues might very well be obviated by future public disclosures by the government and AT&T," but stated that "[i]f necessary, the court may revisit these arguments at a later stage of this litigation." *Id.* at 998. Plaintiffs respectfully submit that if confirmation of the existence of the program by 19 informed members of Congress is not sufficient to obviate these issues, it is time for the Court to address them.

VI. THE COURT'S RULINGS ON AT&T'S MOTION TO DISMISS ARE EQUALLY APPLICABLE HERE

A. Plaintiffs Have Standing to Pursue Their Claims

In *Hepting*, AT&T argued that plaintiffs had "not sufficiently alleged injury-in-fact" to establish standing under the "case or controversy" requirement of Article III of the U.S. Constitution, and that plaintiffs lacked standing to pursue their federal statutory claims "'because the FAC alleges no *facts* suggesting that their statutory rights have been violated' and 'the FAC alleges nothing to suggest that the *named plaintiffs* were themselves subject to surveillance.'" *Id.* at 1000 (emphasis in original). The Court rejected these arguments, and held that plaintiffs had established both Article III standing and standing to pursue their federal statutory claims, on grounds equally applicable here:

> AT&T ignores that the gravamen of plaintiffs' complaint is that AT&T has created a dragnet that collects the content and records of its customers' communications. The court cannot see how any one plaintiff will have failed to demonstrate injury-in-fact if that plaintiff effectively demonstrates that all class members have so suffered. . . . As long as the named plaintiffs were, as they allege, AT&T customers during the relevant time period, the alleged dragnet would have imparted a concrete injury on each of them. [¶] This conclusion is not altered simply because the alleged injury is widely shared among AT&T customers.

Id. at 1000. The only other court to examine the standing issue reached the same conclusion. *See Terkel*, 441 F. Supp. 2d at 904 (allegations based on media reports "that the government intends to collect and analyze all domestic telephone records, that AT&T has already released large quantities of records, and that federal intelligence gathering agencies have focused on their efforts on large metropolitan areas like Chicago . . . sufficiently alleged that [plaintiffs] are suffering a particularized injury for which they can seek relief," and claimed "ongoing violation of [plaintiffs'] statutory rights under section 2702(a)(3) . . . in itself is sufficient to establish standing").

In *Hepting,* AT&T further argued "that the state secrets privilege bars plaintiffs from establishing standing." 439 F. Supp. 2d at 1001. The Court rejected this argument as well, on grounds equally applicable here:

> [A]s described above, the state secrets privilege will not prevent

> plaintiffs from receiving at least some evidence tending to establish the factual predicate for the injury-in-fact underlying their claims directed at AT&T's alleged involvement in the monitoring of communication content. And the court recognizes that additional facts might very well be revealed during, but not as a direct consequence of, this litigation that obviate many of the secrecy concerns currently at issue regarding the alleged communication records program. Hence, it is unclear whether the privilege would necessarily block AT&T from revealing information about its participation, if any, in that alleged program.

Id. at 1001 (internal citations omitted).

B. Plaintiffs Have Alleged the Absence of a Certification

In *Hepting,* AT&T argued that "telecommunications providers are immune from suit if they receive a government certification [under 18 U.S.C. § 2511(2)(a)(ii) or 18 U.S.C. § 2703(e)] authorizing them to conduct electronic surveillance," and "that plaintiffs have the burden to plead affirmatively that AT&T lacks such a certification and that plaintiffs have failed to do so here, thereby making dismissal appropriate." *Id.* at 1001 (citation omitted). The Court rejected this argument, finding that:

> [T]he court need not decide whether plaintiffs must plead affirmatively the absence of a certification because the present complaint, liberally construed, alleges that AT&T acted outside the scope of any government certification it might have received.
>
> * * *
>
> Plaintiffs contend that the phrase "occurred without judicial or other lawful authorization" means that AT&T acted without a warrant or a certification. . . . [¶] . . . [P]aragraph 81 could be reasonably interpreted as alleging just that.
>
> * * *
>
> In sum, even if plaintiffs were required to plead affirmatively that AT&T did not receive a certification authorizing its alleged actions, plaintiffs' complaint can fairly be interpreted as alleging just that.

Id. at 1002-03.[66]

As set forth above, in *Hepting*, the dispute focused on whether or not plaintiffs

[66] Plaintiffs respectfully disagree with the Court's suggestion that "a lack of certification is an element of a Title III claim" under 18 U.S.C. § 2520 (*id.* at 1002), as opposed to an affirmative defense, and incorporate by reference the *Hepting* plaintiffs' briefing and argument on this issue as if fully set forth herein. However, as it is equally unnecessary to resolve this issue here, Plaintiffs will not burden the Court with such unnecessary and/or duplicative briefing.

had *implicitly* alleged that AT&T had not received a certification under either 18 U.S.C. § 2511(2)(a)(ii) or 18 U.S.C. § 2703(e). Here, Plaintiffs have *expressly* alleged the absence of any such certification.[67] Because the *Hepting* plaintiffs' *implicit* allegation was sufficient to pass muster, *a fortiori*, Plaintiffs' *explicit* allegations that Defendants did not receive certifications also suffice.

C. Defendants Have No Common Law Immunity

In *Hepting*, AT&T argued that "the complaint should be dismissed because it failed to plead the absence of an absolute common law immunity to which AT&T claims to be entitled." *Id.* at 1003. The Court rejected this argument as well, concluding that:

> [E]ven if a common law immunity existed decades ago, applying it presently would undermine the carefully crafted scheme of claims and defenses that Congress established in subsequently enacted statutes. For example, all of the cases cited by AT&T as applying the common law "immunity" were filed before the certification provision of FISA went into effect. That provision protects a telecommunications provider from suit if it obtains from the Attorney General or other authorized government official a written certification "that no warrant or court order is required by law, that all statutory requirements have been met, and that the specified assistance is required." 18 U.S.C. § 2511(2)(a)(ii)(B). Because the common law "immunity" appears to overlap considerably with the protections afforded under the certification provision, the court would in essence be nullifying the procedural requirements of that statutory provision by applying the common law "immunity" here. And given the shallow doctrinal roots of immunity for communications carriers at the time Congress enacted the statutes in play here, there is simply no reason to presume that a common law immunity is available simply because Congress has not expressed a contrary intent.

Id. at 1005-06 (citations omitted).

The Court's holding that recognizing a common law immunity for telecommunications carriers "would undermine the carefully crafted scheme of claims and defenses that Congress established in subsequently enacted statutes" is a pure conclusion of law, and is therefore equally applicable here.

---

[67] *See* MCI/Verizon Master Compl., ¶ 209 ("Defendant has not been provided with a certification in writing by a person specified in 18 U.S.C. § 2518(7) or by the Attorney General of the United States meeting the requirements of 18 U.S.C. § 2511(2)(a)(ii)(B), *i.e.*, a certification that no warrant or court order authorizing the disclosures is required by law, and that all statutory requirements have been met."); Bellsouth Master Compl., ¶ 109 (same); Sprint Master Compl., ¶ 81 (same); Transworld Master Compl., ¶ 96 (same); Cingular Master Compl., ¶ 97 (same).

D. **Defendants Have No Qualified Immunity**

In *Hepting*, AT&T argued that "it is entitled to qualified immunity." *Id*. at 1006. After reviewing at length the history and purposes of the qualified immunity doctrine, the Court concluded that:

> AT&T's concerns, while relevant, do not warrant extending qualified immunity here because the purposes of that immunity are already well served by the certification provision of 18 U.S.C. § 2511(2)(a)(ii).
>
> More fundamentally, "[w]hen Congress itself provides for a defense to its own cause of action, it is hardly open to the federal court to graft common law defenses on top of those Congress creates." *Berry v. Funk*, 146 F.3d 1003, 1013 (D.C. Cir. 1998) (holding that qualified immunity could not be asserted against a claim under Title III). . . .
>
> [T]he statutes in this case set forth comprehensive, free-standing liability schemes, complete with statutory defenses, many of which specifically contemplate liability on the part of telecommunications providers such as AT&T. . . . It can hardly be said that Congress did not contemplate that carriers might be liable for cooperating with the government when such cooperation did not conform to the requirements of the act.
>
> In sum, neither the history of judicially created immunities for telecommunications carriers nor the purposes of qualified immunity justify allowing AT&T to claim the benefit of the doctrine in this case.

Id. at 1008-09. The Court's reasoning, as well as its conclusion, is equally applicable here, as it depends not on allegations unique to AT&T, but on an analysis of statutory framework.

The Court further held that:

> AT&T is not entitled to qualified immunity with respect to plaintiffs' constitutional claim, at least not at this stage of the proceedings. Plaintiffs' constitutional claim alleges that AT&T provides the government with direct and indiscriminate access to the domestic communications of AT&T customers. . . . Accordingly, AT&T's alleged actions here violate the constitutional rights clearly established in *Keith*.[68] Moreover, because "the very action in question has previously been held unlawful," AT&T cannot seriously contend that a reasonable entity in its position could have believed that the alleged domestic dragnet was legal. [¶] Accordingly, the court DENIES AT&T's instant motion to dismiss on the basis of qualified immunity.

Id. at 1009-10 (quoting *Hope v. Pelzer*, 536 U.S. 730, 739 (2002)).

---

[68] *United States v. United States District Court*, 407 U.S. 297 (1972).

As in *Hepting*, Plaintiffs have alleged that Defendants have provided the federal government with "indiscriminate access to the domestic communications" of their customers, as well as records pertaining to those communications. Accordingly, as in *Hepting*, Defendants are not entitled to qualified immunity on Plaintiffs' constitutional claim.

VII. CONCLUSION

For the foregoing reasons, the Court's rulings in *Hepting* should apply to the cases brought against the other Defendants, except the Court should find that the existence of the records program, and AT&T's and MCI's participation in the program, is no longer a secret, and permit discovery on Plaintiffs' records claims.

Dated: February 1, 2007

Respectfully submitted,

LIEFF, CABRASER, HEIMANN & BERNSTEIN, LLP

By: *\s\ Barry R. Himmelstein*
Barry R. Himmelstein
Interim Class Counsel for MCI Class

Ronald L. Motley
Jodi W. Flowers
Don Migliori
Vincent Parrett (State Bar No. 237563)
Justin B. Kaplan
MOTLEY RICE, LLC
28 Bridgeside Boulevard
P.O. Box 1792
Mount Pleasant, SC 29465
Telephone: (843) 216-9000
Facsimile: (843) 216-9027

Interim Class Counsel For Verizon Class and Transworld Class

Clinton A. Krislov
W. Joel Vander Vliet
KRISLOV & ASSOCIATES, LTD.
20 North Wacker Drive
Suite 1350
Chicago, IL 60606
Telephone: (312) 606-0500
Facsimile: (312) 606-0207

BRUCE I. AFRAN, ESQ.
10 Braeburn Drive
Princeton, NJ 08540
Telephone: (609) 924-2075

Carl J. Mayer
MAYER LAW GROUP
66 Witherspoon Street, Suite 414
Princeton, NJ 08542
Telephone: (609) 921-8025
Facsimile: (609) 921-6964

Val Patrick Exnicios
LISKA, EXNICIOS & NUNGESSER
ATTORNEYS-AT-LAW
One Calan Place, Suite 2290
365 Canal Street
New Orleans, LA 70130
Telephone: (504) 410-9611
Telephone: (504) 410-9937

Steven E. Schwarz
THE LAW OFFICES OF STEVEN E. SCHWARZ, ESQ.
2461 W. Foster Ave., #1W
Chicago, IL 60625
Telephone: (773) 837-6134
Facsimile: (773) 837-6134

Interim Class Counsel for Bellsouth Class

Gary E. Mason
Nicholas A. Migliaccio
THE MASON LAW FIRM, P.C.
1225 19th Street, NW
Suite 500
Washington, DC 20038
Telephone: (202) 429-2290
Facsimile: (202) 429-2294

John C. Whitfield
WHITFIELD & COX PSC
29 East Center ST.
Madisonville, KY 42431
Telephone: (270) 821-0656
Facsimile: (270) 825-1163

Interim Class Counsel for Sprint Class

R. James George, Jr.
Douglas Brothers
GEORGE & BROTHERS, L.L.P.
1100 Norwood Tower
114 W. 7th Street
Austin, TX 78701
Telephone: (512) 495-1400
Facsimile: (512) 499-0094

Interim Class Counsel For Cingular Class

Ann Brick (State Bar No. 65296)
Nicole A. Ozer (State Bar No. 228643)
AMERICAN CIVIL LIBERTIES UNION FOUNDATION OF NORTHERN CALIFORNIA
39 Drumm Street
San Francisco, CA 94111
Telephone: (415) 621-2493
Facsimile: (415) 255-8437

Laurence F. Pulgram (State Bar No. 115163)
Mitchell Zimmerman (State Bar No. 88456)
Jennifer L. Kelly (State Bar No. 193416)
Saina Shamilov (State Bar No. 215636)
Candace Morey (State Bar No. 233081)
FENWICK & WEST LLP
555 California Street
San Francisco, CA 94104
Telephone: (415) 875-2300
Facsimile: (415) 281-1350

Attorneys for Plaintiffs in *Campbell v. ATT Communications of California,* C-06-3596 VRW, and *Riordan v. Verizon Communications, Inc.*, C-06-3574 VRW

Pursuant to General Order 45, Part X-B, the filer attests that concurrence in the filing of this document has been obtained from Jodi W. Flowers, Clinton A. Krislov, Val Patrick Exnicios, Steven E. Schwarz, Bruce I. Afran, Carl J. Mayer, Gary E. Mason, John C. Whitfield, R. James George, Jr., Ann Brick, and Laurence F. Pulgram.